



State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
137	A	Domain Name System (DNS)	8/15/2013	1 of 3

1.0 PURPOSE

DNS (Domain Naming System) resolution is very important to the communication and connectivity of State computers and devices within the State of Nevada's Silvernet. All agency DNS domain and network segment information within the State of Nevada's Silvernet must be reliably and accurately resolvable by the servers of the State of Nevada DNS System. The purpose of this standard is to establish the requirements for DNS systems and settings that are to be used by State agencies within Silvernet.

2.0 SCOPE

This standard applies to all State agencies who maintain their own DNS/Directory services and/or systems within Silvernet.

3.0 EFFECTIVE DATES

This standard becomes effective at the time of approval of the State Chief Information Officer (CIO).

4.0 RESPONSIBILITIES

The agency head and appointed agency Information Security Officer (ISO) have the responsibility to ensure the implementation of and compliance with this standard.

5.0 RELATED DOCUMENTATION

- <http://nerds.state.nv.us/dns.htm>
- http://en.wikipedia.org/wiki/Domain_Name_System

6.0 STANDARDS

- 1) Within Silvernet EITS highly recommends that agencies that have their systems in "resource" child domains of the State of Nevada Active Directory Forest, and that those child domains contain DNS servers that the agencies have their systems solely pointed to for DNS resolution. Agency DNS servers should be configured to point to the State's internal DNS servers as "Forwarders" for resolution of all DNS information other than their own. If the agency's DNS servers are in Northern Nevada, then they must be configured to point to "ns1.state.nv.us" and "ns2.state.nv.us" as Forwarders. If the agency's DNS servers are in Southern Nevada, then they must be configured to point to "ns4.state.nv.us" and "ns5.state.nv.us" as Forwarders. The Forward and Reverse Lookup Zones for the agency domains and network segments must be configured as "Active Directory Integrated" zones, so that they will replicate automatically with the DNS servers of the State of Nevada DNS System.
- 2) Alternatively, agencies can have their own Directories which contain DNS servers that their systems are solely pointing to for DNS resolution. Agency DNS servers must be configured to point to the State's internal DNS servers as Forwarders for resolution of all DNS information other



State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
137	A	Domain Name System (DNS)	8/15/2013	2 of 3

than their own. If the agency's DNS servers are in Northern Nevada, then they must be configured to point to "ns1.state.nv.us" and "ns2.state.nv.us" as Forwarders. If the agency's DNS servers are in Southern Nevada, then they must be configured to point to "ns4.state.nv.us" and "ns5.state.nv.us" as Forwarders.

- 3) Within Silvernet all agency systems must have their "Connection-specific DNS suffix" set to the agency domain.
- 4) Within Silvernet all agency systems must have their DNS suffix search list configured to point to the following domains in the order that they're listed: 1) The agency's domain 2) Any domains that the agency has a trust with, that they share resources with, and/or any child domains 3) "state.nv.us" 4) "nv.gov" 5) "nevada.gov".
- 5) Within Silvernet all agency systems must have their "Primary DNS Suffix", which is part of the system's full computer name, set to the agency domain.
- 6) The Forward and Reverse Lookup Zones for agency domains and network segments must be configured to allow Zone Transfers to the State of Nevada DNS System's primary DNS server. Agencies must monitor their DNS server logs to make sure that Zone Transfers to the State of Nevada DNS System's primary DNS server are working reliably for their Forward and Reverse Lookup Zone domain(s) and network segments. In the event that Zone Transfers stop working for any of an agency's Forward and Reverse lookup zones to the State of Nevada DNS System's primary DNS server, the agency must get those Zone Transfers working again within 48 hours and must let the State of Nevada Internet Services and Servers Group (sig@admin.nv.gov) know when they've been restored.

7.0 DEFINITIONS

State agency: Any State of Nevada Government entity (Department, Division, Board, Commission, Committee, etc.).

Systems: Mainframes, servers, PC's, laptops, tablets, printers, scanners, and other computing devices that have configurable DNS settings and that are connected to Silvernet.

State of Nevada DNS System servers on Silvernet:

- ns1.state.nv.us = 10.131.11.24 (Primary Northern Nevada DNS server)
- ns2.state.nv.us = 10.131.11.25 (Secondary Northern Nevada DNS server)
- ns3.state.nv.us = 10.131.11.126
- ns4.state.nv.us = 10.231.86.126 (Primary Southern Nevada DNS server)
- ns5.state.nv.us = 10.231.86.127 (Secondary Southern Nevada DNS server)
- ns6.state.nv.us = 10.131.11.146

8.0 EXCEPTIONS/OTHER ISSUES

Requests for exception to the requirements of this Information Security Standard must be documented, provided to the Office of Information Security (OIS), and approved by the State Chief Information Security Officer (CISO).



State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
137	A	Domain Name System (DNS)	8/15/2013	3 of 3

Approved By		
Title	Signature	Date
State Information Security Committee	Approved by Committee	07/25/2013
State Chief Information Security Officer (CISO)	Signature on File	10/22/2014
State Chief Information Officer (CIO)	Signature on File	10/22/2014

Document History		
Revision	Date	Change
A		Initial release.